Lab 239

Morris & Opazo

aws re/start

Amazon Linux

# Procesos administrativo

# INTRODUCCIÓN

La administración de procesos en Linux es una parte crítica de la gestión del sistema operativo. Un proceso es cualquier programa en ejecución, y la capacidad de gestionar estos procesos de manera eficiente es esencial para mantener un sistema saludable y optimizado. Desde monitorear el rendimiento hasta controlar el uso de recursos, la administración de procesos permite a los administradores de sistemas garantizar que las aplicaciones se ejecuten sin problemas y que el sistema responda adecuadamente a las demandas.

# OBJETIVOS

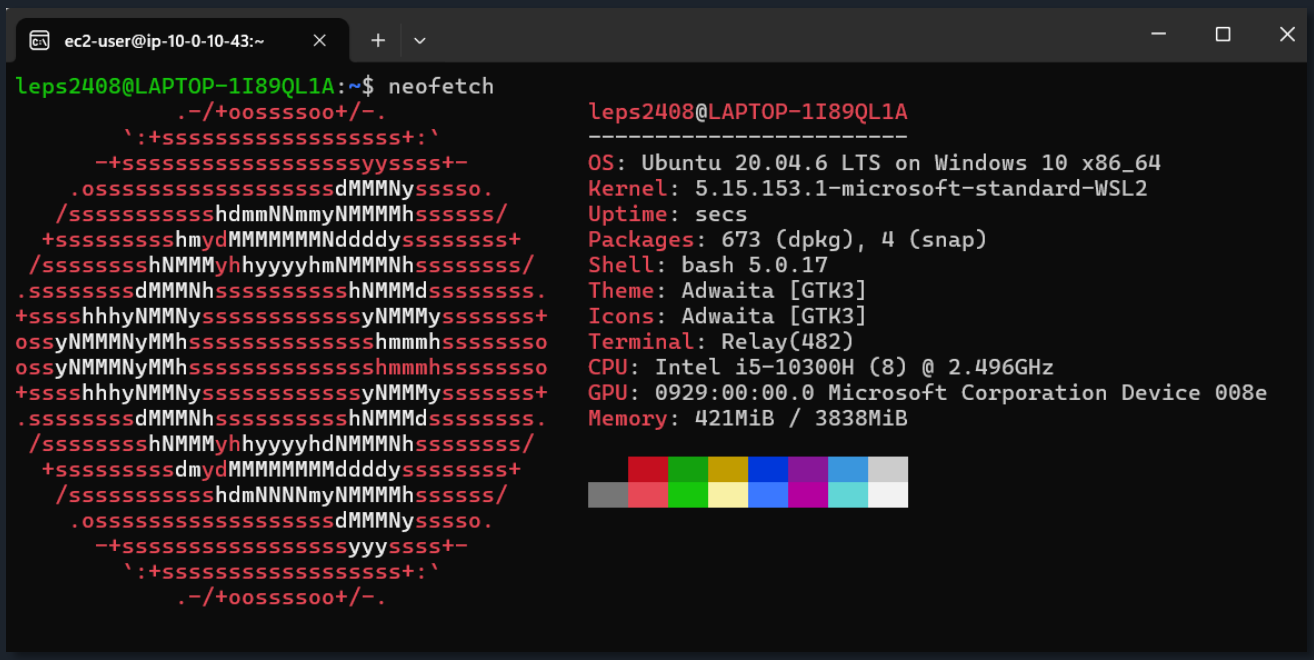
- Crear un archivo de registro nuevo para las listas de procesos.
- Utilizar el comando *top*.
- Establecer una tarea repetitiva que ejecute los comandos de auditoría anteriores una vez al día.

# TAREA 1

En esta tarea, se conectará a una instancia EC2 de Amazon Linux. Utilizará una utilidad SSH para realizar todas estas operaciones. Las siguientes instrucciones varían ligeramente según si utiliza Windows o Mac/Linux.

## En Linux

- Usando distribución Ubuntu con Subsistema de Windows para Linux (WSL).



- Ubicarse en la carpeta del archivo *labuser.pem* descargado.

```
leps2408@LAPTOP-1I89QL1A:~$ ls
labsuser.pem  labsuser.pem:Zone.Identifier
```

- Cambiar permisos a *labuser.pem* descargado, según el comando.

```
leps2408@LAPTOP-1I89QL1A:~$ chmod 400 labsuser.pem
```

- Conectar con la instancia EC2 de AWS utilizando el IP público IPv4, según el comando.

```
leps2408@LAPTOP-1I89QL1A:~$ ssh -i labsuser.pem ec2-user@35.94.49.146
The authenticity of host '35.94.49.146 (35.94.49.146)' can't be established.
ECDSA key fingerprint is SHA256:ropSTchpGPT/u0xCZgDNMY4VOD2vvauVnHu+KovTfGI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.94.49.146' (ECDSA) to the list of known hosts.
```

- Finalmente, se muestra la imagen de la distribución de Amazon Linux 2.

```
       #_
       ~\_  ####_        Amazon Linux 2
      ~~  \_#####\
      ~~     \###|       AL2 End of Life is 2025-06-30.
      ~~       \#/ ___
       ~~       V~' '->
        ~~~         /    A newer version of Amazon Linux is available!
          ~~._.   _/
             _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
           _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/
```

# TAREA 2

En este ejercicio, se crea un archivo de registro a partir del comando *ps*. Ese archivo de registro debe agregarse a la sección SharedFolders. Cree un archivo de registro denominado processes.csv con *ps -aux* y omita cualquier proceso que contenga un usuario raíz "[" o "]" en la sección COMMAND.

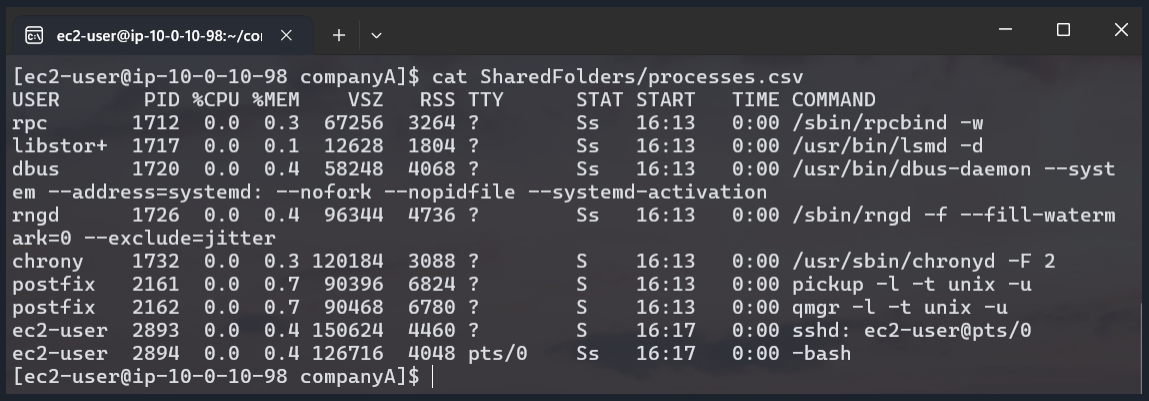
- Asegurarse de estar en la carpeta CompanyA.

```
ec2-user@ip-10-0-10-98:~/co
[ec2-user@ip-10-0-10-98 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-98 ~]$ cd companyA/
[ec2-user@ip-10-0-10-98 companyA]$
```

- Mirar los procesos que se encuentran corriendo y filtrar la palabra raíz escribiendo *sudo ps -aux | grep -v root | sudo tee SharedFolders/processes.csv*.

```
ec2-user@ip-10-0-10-98:~/co
[ec2-user@ip-10-0-10-98 companyA]$ sudo ps -aux | grep -v root | sudo tee SharedFolders/proc
esses.csv
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
rpc        1712  0.0  0.3  67256  3264 ?        Ss   16:13   0:00 /sbin/rpcbind -w
libstor+   1717  0.0  0.1  12628  1804 ?        Ss   16:13   0:00 /usr/bin/lsmd -d
dbus       1720  0.0  0.4  58248  4068 ?        Ss   16:13   0:00 /usr/bin/dbus-daemon --syst
em --address=systemd: --nofork --nopidfile --systemd-activation
rngd       1726  0.0  0.4  96344  4736 ?        Ss   16:13   0:00 /sbin/rngd -f --fill-waterm
ark=0 --exclude=jitter
chrony     1732  0.0  0.3 120184  3088 ?        S    16:13   0:00 /usr/sbin/chronyd -F 2
postfix    2161  0.0  0.7  90396  6824 ?        S    16:13   0:00 pickup -l -t unix -u
postfix    2162  0.0  0.7  90468  6780 ?        S    16:13   0:00 qmgr -l -t unix -u
ec2-user   2893  0.0  0.4 150624  4460 ?        S    16:17   0:00 sshd: ec2-user@pts/0
ec2-user   2894  0.0  0.4 126716  4048 pts/0    Ss   16:17   0:00 -bash
[ec2-user@ip-10-0-10-98 companyA]$
```

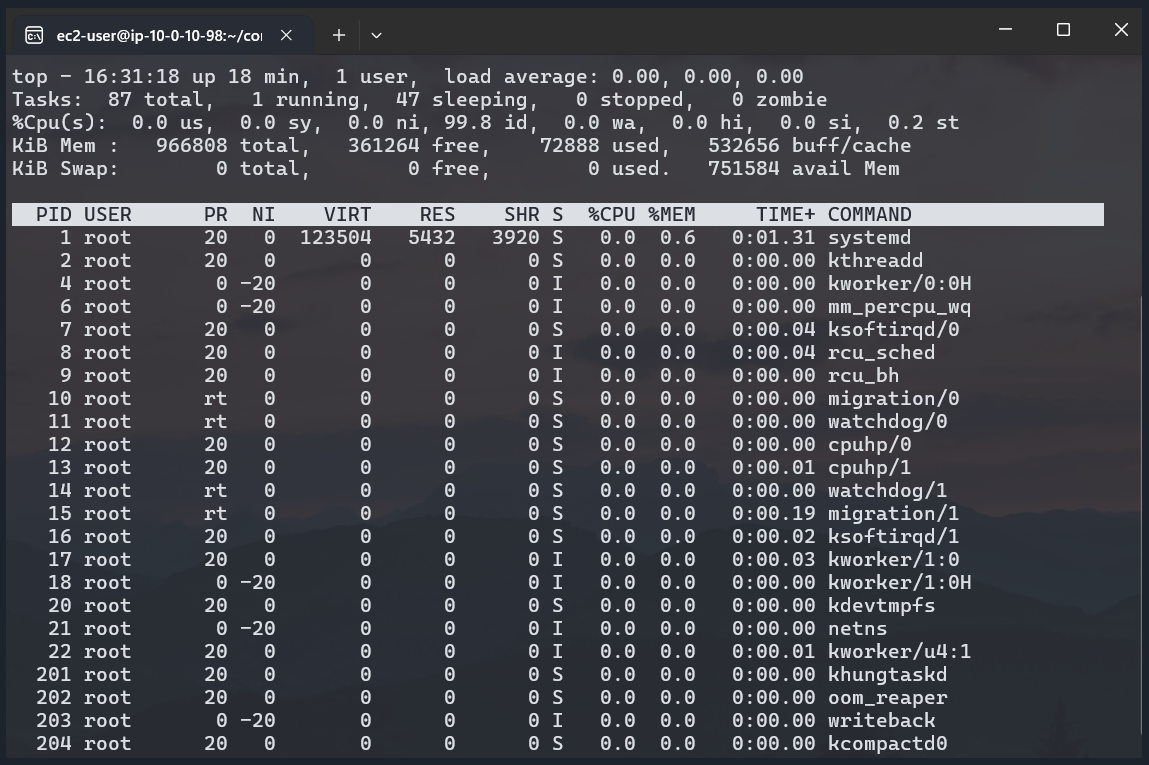
- Confirmar con *cat SharedFolders/processes.csv*.



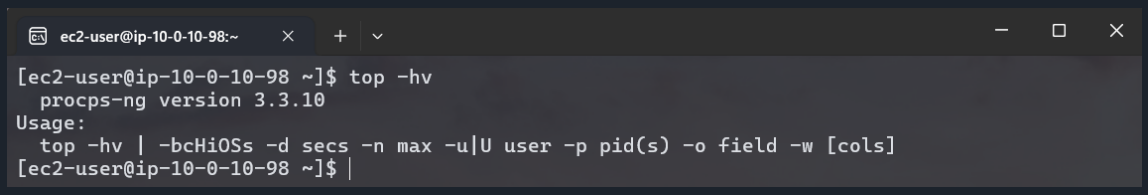
# TAREA 3

En este ejercicio, se utilizará el comando *top*. Ejecutar el comando *top* para mostrar los procesos e hilos que están activos en el sistema y observar las salidas con el comando *top*.

- Ingresar el comando *top*. Nota: 87 tareas se encuentran en total, 1 (running), 47 (sleeping)



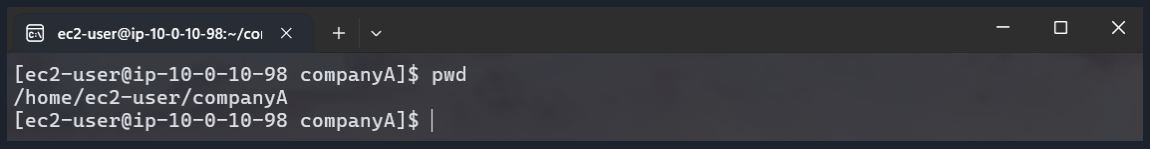

- Para salir, presionar *q*. Probar el comando *top –hv* para encontrar información de uso y versión.


ec2-user@ip-10-0-10-98:~
[ec2-user@ip-10-0-10-98 ~]$ top -hv
procps-ng version 3.3.10
Usage:
top -hv | -bcHiOSs -d secs -n max -u|U user -p pid(s) -o field -w [cols]
[ec2-user@ip-10-0-10-98 ~]$

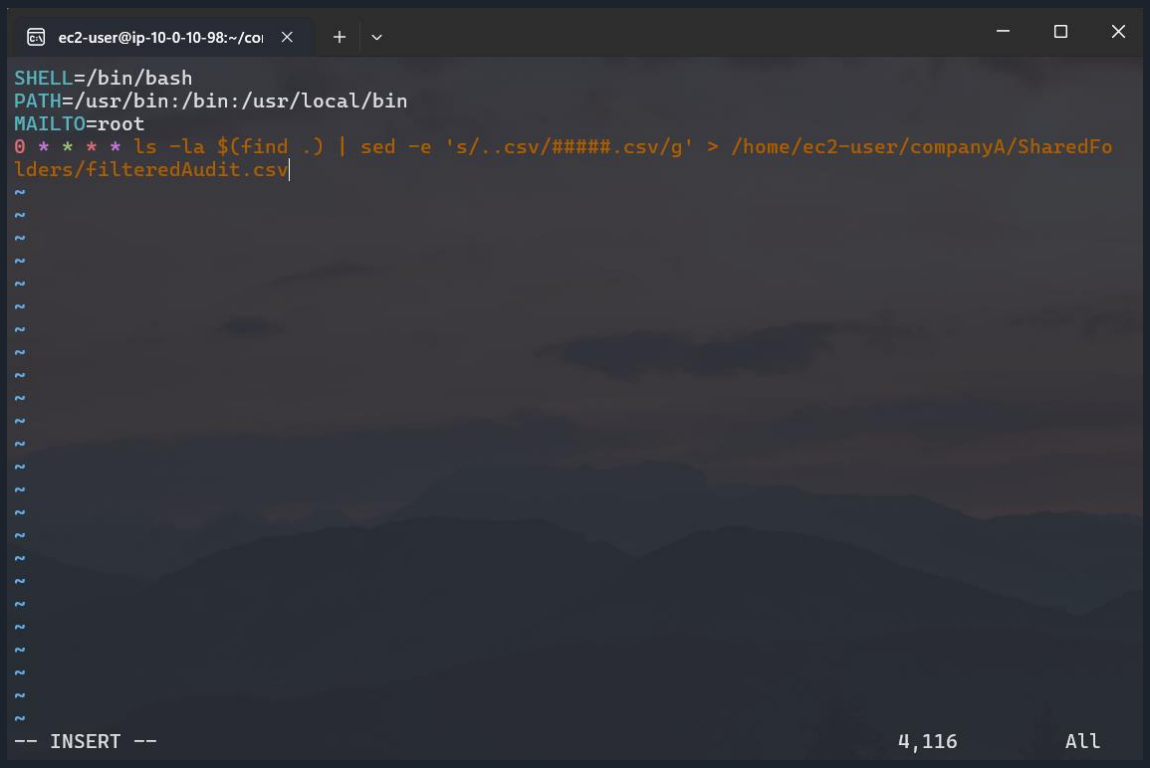
# TAREA 4

En este ejercicio, creará un trabajo cron que generará un archivo de auditoría con ##### para cubrir todos los archivos .csv. Recuerde que cron es un comando que ejecuta una tarea de forma regular a una hora determinada

- Validar que se encuentra en la carpeta CompanyA, ingresar *pwd*.




- Ingresar *sudo crontab –e* para crear un espacio de trabajo. Ingresar al modo de inserción. Ingresar *SHELL=/bin/bash,* luego *PATH=/usr/bin:/bin:/usr/local/bin*, en la siguiente línea *MAILTO=root*, y finalmente en la última línea se ingresa *0 * * * * ls -la $(find .) | sed -e 's/..csv/#####.csv/g' > /home/ec2-user/companyA/SharedFolders/filteredAudit.csv*




- Guardar el archivo y confirmar con *sudo crontab –l*.